UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/716,221	11/21/2000	Hisashi Inoue	2000 1451A	9406

7590 05/06/2004

Wenderoth Lind & Ponack LLP
2033 K Street NW
Suite 800
Washington, DC 20006

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 05/06/2004 5

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/716,221	**Applicant(s)** INOUE ET AL.	
	Examiner Pramila Parthasarathy	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on *01 April 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *#2 and #4*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on 4/01/2003. Claims 1 – 18 were received for consideration. No preliminary amendments to the specification were filed. Claims 1 – 18 are currently being considered.

Claim Objections

2. Claim 5 is objected to because of the following informalities:

Delete the word "is" from Claim 5 line 5.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1- 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakamura et al. (U.S. Patent No. 6,185,312) in view of Barton (U.S. Patent No. 6,047,374 hereinafter "Barton").

Regarding Claim 1, Nakamura teaches and describes a tamper-detection-information embedding apparatus for embedding predetermined information for tamper detection in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), comprising:

band division means for dividing said digital image signal into a plurality of frequency bands (Fig. 2 #11 and Column 5 lines 42 – 44);

authentication data generation means for generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series (Fig. 3 # 31 and Column 5 lines 42 – 55);

key data embedding means for embedding said key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands (Fig. 3 #22, 23 and Column 6 lines 4 – 57);

authentication data embedding means for embedding said authentication data in transform coefficients of the frequency bands exclusive of said MRA (hereinafter, referred to as MRR) among said plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 – Column 17 line 46); and

band synthesis means for reconstructing the digital image signal in which the information has been embedded by using said MRA and said MRR to which data embedding processing is subjected (Fig. 2, 6 – 12; Column 8 line 45 – Column 11 line 16, Column 15 line 25 – Column 18 line 57 and Fig. 51 – 54, Column 38 line 42 – Column 39 line 25).

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding authentication information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 3, Nakamura teaches and describes a tamper detection apparatus for detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), comprising:

band division means for dividing said digital image signal into a plurality of frequency bands (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43);

authentication data generation means for generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series (Fig. 3 # 31 and Column 5 lines 42 – 55);

key data embedded by said specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands (Fig. 3 # 22, 23 and Column 6 lines 4 – 57). Nakamura does not explicitly disclose key data extraction means for extracting said key data embedded by said specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands. However Barton discloses a method and apparatus for generating, embedding and extracting authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28),

embedded information extraction means for extracting embedded information embedded based on said key data by said specific apparatus from transform coefficients of the frequency bands exclusive of said MRA (hereinafter, referred to as MRR) among said plurality of frequency bands (Barton Fig. 2 # 42, Column 4 lines 22 – 41 and Column 7 line 55 – Column 8 line 28); and

tamper determination means for comparing said embedded information with said authentication data for verification and determining whether said digital image has been tampered with (Barton Fig. 2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate, embed and extract the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding and extracting digital image with authentication information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 7, Nakamura teaches and describes a tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), comprising:

a step of dividing said digital image signal into a plurality of frequency bands (Fig. 2 # 11 and Column 5 lines 42 – 44);

a step of generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series (Fig. 3 #31 and Column 5 lines 42 – 55);

a step of embedding said key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands (Fig. 3 and Column 6 lines 4 – 57);

a step of embedding said authentication data in transform coefficients of the frequency bands exclusive of said MRA (hereinafter, referred to as MRR) among said plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 – Column 17 line 46);

a step of reconstructing the digital image signal in which the information has been embedded by using said MRA and said MRR to which data embedding processing is subjected (Fig. 2, 6 – 12; Column 8 line 45 – Column 11 line 16 and Fig. 51 – 54, Column 38 line 42 – Column 39 line 25).

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding authentication information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 9, Nakamura teaches and describes a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), comprising:

a step of dividing said digital image signal into a plurality of frequency bands (Fig. 2 #11 and Column 5 lines 42 – 44);

a step of key data embedded by said specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands (Fig. 3 # 22, 23 and Column 6 lines 4 – 57). Nakamura does not explicitly disclose a step of extracting key data extraction means for extracting said key data embedded by said specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands. However Barton discloses a method and apparatus for generating, embedding and extracting authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28),

a step of embedding said authentication data in transform coefficients of the frequency bands exclusive of said MRA (hereinafter, referred to as MRR) among said plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 – Column 17 line 46);

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28);

a step of reconstructing the digital image signal in which the information has been embedded by using said MRA and said MRR to which data embedding processing is subjected (Fig. 2, 6 – 12; Column 8 line 45 – Column 11 line 16, Column 15 line 25 – Column 18 line 57 and Fig. 51 – 54, Column 38 line 42 – Column 39 line 25).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding authentication information.

The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 13, Nakamura teaches and describes a recording medium on which a program to be run on a computer device is recorded for carrying out a tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), the method comprising the steps of:

dividing said digital image signal into a plurality of frequency bands (Fig. 2 #11 and Column 5 lines 42 – 44);

generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series (Fig. 3 # 31 and Column 5 lines 42 – 55);

embedding said key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 – Column 17 line 46);

embedding said authentication data in transform coefficients of the frequency bands exclusive of said MRA (hereinafter, referred to as MRR) among said plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 and Column 17 line 46); and

reconstructing the digital image signal in which the information has been embedded by using said MRA and said MRR to which data embedding processing is subjected (Fig. 2, 6 – 12; Column 8 line 45 – Column 11 line 16, Column 15 line 25 – Column 18 line 57 and Fig. 51 – 54, Column 38 line 42 – Column 39 line 25).

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding authentication information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 15, Nakamura teaches and describes a recording medium on which a program to be run on a computer device is recorded for carrying out a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), the method comprising the steps of:

dividing said digital image signal into a plurality of frequency bands (Fig. 2 #11 and Column 5 lines 42 – 55);

extracting key data embedded by said specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands;

generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series (Fig. 3 # 31 and Column 5 lines 42 – 55);

key data embedded by said specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands (Fig. 3 # 22, 23 and Column 6 lines 4 – 57). Nakamura does not explicitly disclose key data extraction means for extracting said key data embedded by said specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among said plurality of frequency bands. However Barton discloses a method and apparatus for generating, embedding and extracting authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28), and

comparing said embedded information with said authentication data for verification and determining whether said digital image has been tampered with (Barton Fig. 2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding authentication information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Nakamura teaches and describes a tamper-detection-information embedding apparatus for embedding predetermined information for tamper detection in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein

a set value T (T is a positive integer) and a set value m (m is an integer not more than T) are predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38); and

said authentication data embedding means embeds said authentication data in each transform coefficient of said MRR by comparing an absolute value of said transform coefficient with said set value T, and if the absolute value is less than said set value T, setting the transform coefficient to said set value +m or –m depending on the bit value of said authentication data to be embedded, and if the absolute value is not less than said set value T, setting the transform coefficient to an even or odd integer nearest to said value q depending on the bit value of said authentication data to be embedded (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Nakamura teaches and describes a tamper detection apparatus for detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein

said tamper determination means comprises:

block division means for dividing the digital image into a plurality of unit blocks each composed on a predetermined number of pixels (Fig. 2 # 11, Column 5 lines 42 – 44; Fig. 9, Column 14 line 61 – Column 15 line 55, Fig. 12, 13, Column 17 lines 21 – 32 and Fig. 25, 26, Column 23 lines 15 – 46);

regional embedded information read means for reading, for each of said unit blocks, embedded information embedded in the transform coefficients of said MRR that represents the same spatial region as the unit block, serially from all of said embedded information extracted by said embedded information extraction means (Fig. 10, Column 16 lines 17 – 37);

regional authentication data read means for reading, for each of said unit blocks, authentication data corresponding in position to said embedded information serially read by said regional embedded information read means, serially from all of said authentication data generated by said authentication data generation means (Fig. 10, Column 16 lines 17 – 53 and Fig. 35 Column 28 line 5 – Column 29 line 41); and

block-tamper determination means for comparing said embedded information serially read with said authentication data serially read and determining, for each of said unit blocks, whether said digital image has been tampered with (Barton Fig. 2 Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 5 is rejected as applied above in rejecting claim 3. Furthermore, Nakamura teaches and describes a tamper detection apparatus for detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein

a set value T (T is a positive integer) is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38), and

said embedded information extraction means extracts said embedded information from each transform coefficient of said MRR by comparing an absolute value of said transform coefficient with said set value T, and if the absolute value is less than said set value T, determining whether a value of the transform coefficient is positive or negative and extracting a bit value of embedded information in the transform coefficient based on the determination, and if the absolute value is not less than said set value T, determining whether said value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the determination (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Nakamura teaches and describes a tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein

a set value T (T is a positive integer) and a set value m (m is an integer not more than T) are predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38); and

said step of embedding authentication data includes:

a step of comparing an absolute value of said transform coefficient with said set value T, and if the absolute value is less than said set value T;

a step of setting the transform coefficient to said set value +m or –m depending on the bit value of said authentication data to be embedded, and if the absolute value is not less than said set value T; and

a step of setting the transform coefficient to an even or odd integer nearest to said value q depending on the bit value of said authentication data to be embedded if the absolute value is not less than said set value T. (Fig. 17, 48; Column 18 lines 9 –

57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Nakamura teaches and describes a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein

said step of determining tamper comprises:

a step of dividing the digital image into a plurality of unit blocks each composed on a predetermined number of pixels (Fig. 2 # 11, Column 5 lines 42 – 44; Fig. 9, Column 14 line 61 – Column 15 line 55, Fig. 12, 13, Column 17 lines 21 – 32 and Fig. 25, 26, Column 23 lines 15 – 46);

a step of reading, for each of said unit blocks, embedded information embedded in the transform coefficients of said MRR that represents the same spatial region as the unit block, serially from all of said embedded information (Fig. 10, Column 16 lines 17 – 37);

a step of reading, for each of said unit blocks, authentication data corresponding in position to said embedded information serially read, serially from all of said authentication data (Fig. 10, Column 16 lines 17 – 53 and Fig. 35 Column 28 line 5 – Column 29 line 41); and

a step of comparing a series of said embedded formation serially read with a series of said authentication data serially read and determining, for each of said unit blocks, whether said digital image has been tampered with (Barton Fig. 2 Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 11 is rejected as applied above in rejecting claim 9. Furthermore, Nakamura teaches and describes a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein

a set value T (T is a positive integer) is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38), and

said step of extracting embedded information includes:

a step of comparing an absolute value of said transform coefficient with said set value T;

a step of determining whether a value of the transform coefficient is positive or negative if the absolute value is less than said set value T, and extracting a bit value of embedded information in the transform coefficient based on the determination;

a step of determining whether said value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the determination (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore Nakamura teaches and describes a recording medium on which a program to be run on a computer device is recorded for carrying out a tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein

a set value T (T is a positive integer) and a set value m (m is an integer not more than T) are predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38); and

said step of embedding authentication data includes the steps of:

comparing an absolute value of said transform coefficient with said set value T, and if the absolute value is less than said set value T;

setting the transform coefficient to said set value +m or –m depending on the bit value of said authentication data to be embedded, and if the absolute value is not less than said set value T; and

setting the transform coefficient to an even or odd integer nearest to said value q depending on the bit value of said authentication data to be embedded if the absolute value is not less than said set value T. (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Nakamura teaches and describes a recording medium on which a program to be run on a computer device is recorded for carrying out a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein said step of determining tamper comprises the steps of:

dividing the digital image into a plurality of unit blocks each composed on a predetermined number of pixels (Fig. 2 # 11, Column 5 lines 42 – 44; Fig. 9, Column 14 line 61 – Column 15 line 55, Fig. 12, 13, Column 17 lines 21 – 32 and Fig. 25, 26, Column 23 lines 15 – 46);

reading, for each of said unit blocks, embedded information embedded in the transform coefficients of said MRR that represents the same spatial region as the unit block, serially from all of said embedded information (Fig. 10, Column 16 lines 17 – 37);

reading, for each of said unit blocks, authentication data corresponding in position to said embedded information serially read, serially from all of said authentication data (Fig. 10, Column 16 lines 17 – 53 and Fig. 35 Column 28 line 5 – Column 29 line 41); and

comparing a series of said embedded formation serially read with a series of said authentication data serially read and determining, for each of said unit blocks, whether said digital image has been tampered with (Barton Fig. 2 Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 17 is rejected as applied above in rejecting claim 15. Furthermore, Nakamura teaches and describes a recording medium on which a program to be run on a computer device is recorded for carrying out a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein

a set value T (T is a positive integer) is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38), and

said step of extracting embedded information includes the steps of:

comparing an absolute value of said transform coefficient with said set value T;

determining whether a value of the transform coefficient is positive or negative if the absolute value is less than said set value T, and extracting a bit value of embedded information in the transform coefficient based on the determination;

determining whether said value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the determination (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 6 is rejected as applied above in rejecting claim 4. Furthermore, Nakamura teaches and describes a tamper detection apparatus for detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein

a set value T (T is a positive integer) is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38), and

said embedded information extraction means extracts said embedded information from each transform coefficient of said MRR by comparing an absolute value of said transform coefficient with said set value T, and if the absolute value is less than said set value T, determining whether a value of the transform coefficient is positive or negative and extracting a bit value of embedded information in the transform coefficient based on the determination, and if the absolute value is not less than said set value T, determining whether said value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the determination (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 12 is rejected as applied above in rejecting claim 10. Furthermore, Nakamura teaches and describes a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein

a set value T (T is a positive integer) is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38), and

said step of extracting embedded information includes

a step of comparing an absolute value of said transform coefficient with said set value T;

a step of determining whether a value of the transform coefficient is positive or negative if the absolute value is less than said set value T, and extracting a bit value of embedded information in the transform coefficient based on the determination;

a step of determining whether said value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the determination (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 18 is rejected as applied above in rejecting claim 16. Furthermore, Nakamura teaches and describes a recording medium on which a program to be run on a computer device is recorded for carrying out a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein

a set value T (T is a positive integer) is predetermined and q is predetermined as a value obtained by dividing a transform coefficient by a predetermined quantization step size and then rounding off the result (Fig. 17, 48; Column 18 lines 9 – 57 and Column 35 line 25 – Column 37 line 38), and

said step of extracting embedded information includes the steps of:

comparing an absolute value of said transform coefficient with said set value T;

determining whether a value of the transform coefficient is positive or negative if the absolute value is less than said set value T, and extracting a bit value of embedded information in the transform coefficient based on the determination;

determining whether said value q is even or odd and extracting a bit value of embedded information embedded in the transform coefficient based on the determination (Fig. 17, 48; Column 18 lines 9 – 57, Column 35 line 25 – Column 37 line 38; Fig.2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Conclusion

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C. 20231 **or faxed to:** (703) 872-9306 for all formal communications.

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, <u>Fourth Floor</u> (Receptionist).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 703-305-8912. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Pramila Parthasarathy
Patent Examiner
703-305-8912
April 30, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100